



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/695,837

10/30/2003

Tzahi Carmeli

P-5763-US

7206

49444

7590

11/29/2006

PEARL COHEN ZEDEK LATZER, LLP
1500 BROADWAY, 12TH FLOOR
NEW YORK, NY 10036

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/695,837

Applicant(s)

CARMELI, TZAHI

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.


Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 04/05 & 10/03.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. This is in reply to application filed on October 30, 2003. Claims 1-36 have been examined.

Priority

2. This application does not claim priority. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is
10/30/2003.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. **Claims 1-36** are rejected under 35 U.S.C. 102(a) as being anticipated by the Article **submitted with the IDS**, title "Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11:Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements Hereinafter referred as **Draft Amendment**) (IEEE November 2002)
5. **As per independent claims 1, 12, 20, 26 and 32 Draft Amendment** discloses a method comprising: configuring a transmitter and a receiver to encrypt and decrypt, respectively, a data frame based on information included in a header of the data frame.
[See at least figures 26-28 and 33-35]
6. **As per claims 2-3, 13-14, 21-22, 27-28 and 33-34 Draft Amendment** discloses a method as applied to claims above. Furthermore, **Draft Amendment**

Art Unit: 2132

discloses the method further comprising authenticating the header of the data frame and processing the header of the data frame to provide a processed header; and configuring the transmitter and the receiver based on information included in the processed header. [See at least figures 26-28 and 33-35 and also page 53, line 35- page 67 line 25]

7. **As per claims 4-11, 15-19, 23-25, 29-31 and 35-36 Draft Amendment**

discloses a method as applied to claims above. Furthermore, Draft Amendment discloses the method wherein configuring comprises: configuring the receiver to authenticate and decrypt a data portion and a message integrity code portion of the data frame. [See at least figures 26-28 and 33-35] and the method further comprising: decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message integrity code portion, respectively; calculating the message integrity code of the data frame from the decrypted data portion; and comparing the calculated message integrity code to the decrypted message integrity code portion. [See also page 53, line 35-page 67 line 25]

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 1-36** are also rejected under 35 U.S.C. 102(b) as being anticipated by

Callum (Hereinafter referred as **Callum**) (U.S. Patent No. 6,295,604, Patent Date September 25, 2001)

Art Unit: 2132

10. **As per independent claims 1, 12, 20, 26 and 32 Callum Amendment** discloses a method comprising: configuring a transmitter and a receiver to encrypt and decrypt, respectively, a data frame based on information included in a header of the data frame. [See figure 3-5 and at least column 3, lines 25-column 4, line 10]
11. **As per claims 2-3, 13-14, 21-22, 27-28 and 33-34 Callum** discloses a method as applied to claims above. Furthermore, **Callum** discloses the method further comprising authenticating the header of the data frame and processing the header of the data frame to provide a processed header; and configuring the transmitter and the receiver based on information included in the processed header. [See figure 3-5 and at least column 3, lines 25-column 4, line 10]
12. **As per claims 4-11, 15-19, 23-25, 29-31 and 35-36 Callum** discloses a method as applied to claims above. Furthermore, **Callum** discloses the method wherein configuring comprises: configuring the receiver to authenticate and decrypt a data portion and a message integrity code portion of the data frame. [figure 3-5] and the method further comprising: decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message integrity code portion, respectively; calculating the message integrity code of the data frame from the decrypted data portion; and comparing the calculated message integrity code to the decrypted message integrity code portion. [See figure 3-5 and at least column 3, lines 25-column 4, line 10] (Referring now to FIGS. 3-5, data packet 300 includes a header 310 and a data portion 350. In this embodiment, header 310 comprises control information including a control word 320, one or more keys 330 and an initialization vector (IV) 340 as shown in FIG. 4. Control word 320 provides information to control the functionality of CPP unit 230 of FIG. 2. The keys 330 and IV 340 are

Art Unit: 2132

used by CPP unit 230 to perform encryption or decryption operations. And As shown in FIG. 5, one embodiment of control word 320 includes a plurality of bit fields 321-324. These bit fields 321-324 provide the CPP unit with information concerning the length of data packet 300 of FIG. 3, the mode of operation (encryption/decryption), and optionally, the type of cryptographic technique used. It is contemplated that different bit lengths associated bit fields 321-324 may be utilized other than the bit lengths illustrated herein. In particular, as shown in FIGS. 3 and 5, first bit field 321 contains a byte count which indicates the number of bytes in data packet 300, and second bit field 322 includes one or more bits which indicate whether encryption or decryption is to be performed on data portion 350 of the incoming data packet. As optional bit fields of control word 320, third/forth bit fields 323 and 324 indicate the type of cryptographic operation to be performed. For example, if the CPP unit supports DES, third bit field 323 may indicate a selected DES mode (e.g., triple key DES) and fourth bit field 324 may indicate whether Cipher Block Chaining (CBC) or Electronic Codebook (ECB) is desired. The operations associated with CBC and ECB are set forth in a Federal Information Processing Standard Publication (FIPS Pub. 81) entitled "DES Modes of Operation" published on or around Dec. 2, 1980. It is contemplated that other types of cryptographic operations would assign bit fields 323 and 324 to provide different information. Referring back to FIGS. 2 and 4, header 310 further includes keys 330 and IV 340. In this embodiment, three (3) keys are provided, each key being at least 56-bits in length, although any bit size may be used so long as it is in accordance to the cryptographic standard followed by CPP unit 230. In the event that a 32-bit data bus is implemented between memory controller 220 and CPP unit 230, two data transfers maybe employed, in this embodiment to transfer one of the keys 330 as shown in FIG. 4. Initialization vector (IV) 340 is a binary vector used as a randomizing block of data that is exclusively OR'ed (XOR) with a first data block in CBC mode. Finally the following has been disclosed, "Referring back to FIG. 3, data portion 350 includes N data blocks 360.sub.1 -360.sub.N, where "N" is a positive whole number. In this embodiment, a "block" is a

Art Unit: 2132

32-bit word. The sizing of the word is constrained by the bit width of the cryptographic bus situated between memory controller 220 and CPP unit 230 of FIG. 2.")

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

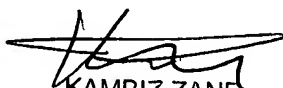
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

11/20/2006

AM 2132


KAMBIZ ZAND
PRIMARY EXAMINER